Multihop Federations & Trust Router

draft-mrw-abfab-multihop-fed-02.txt
draft-mrw-abfab-trust-router-01.txt

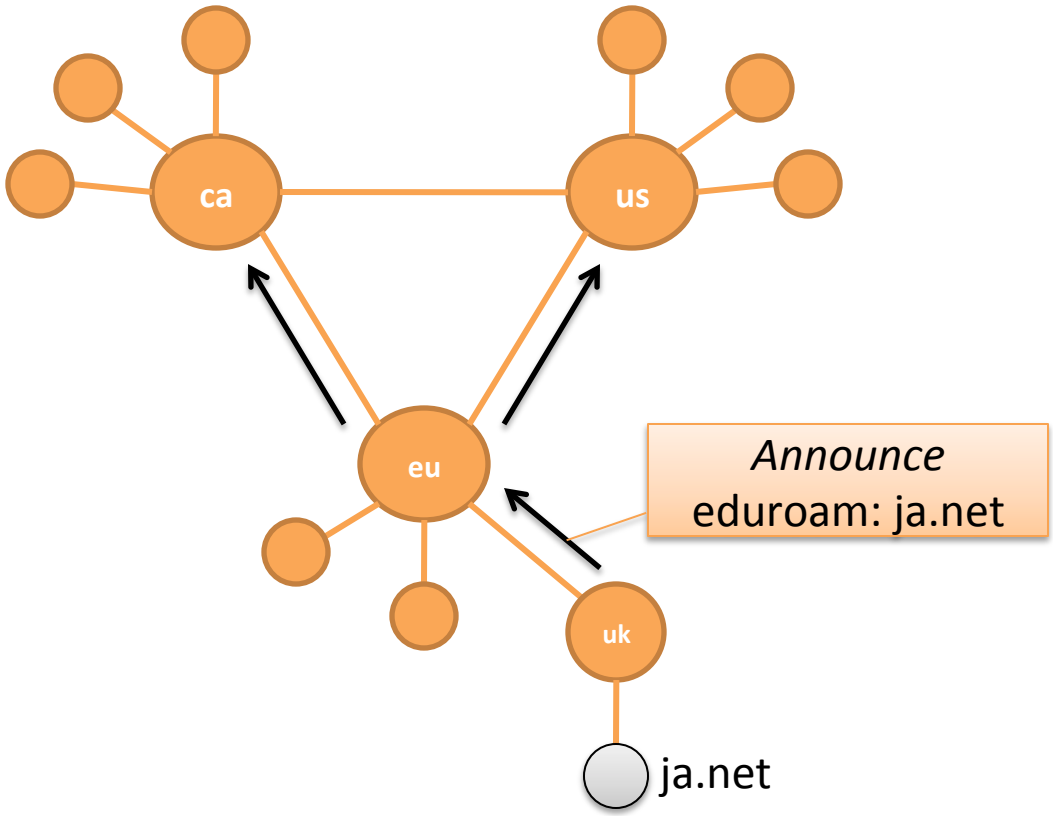
Margaret Wasserman

mrw@painless-security.com

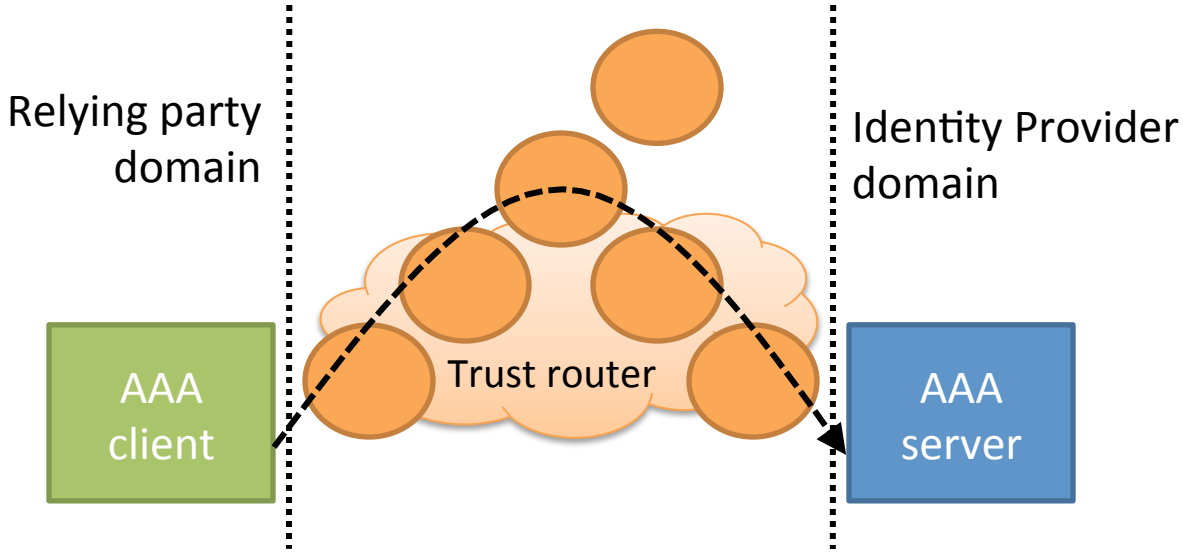
Multihop Federations

- Drafts describe a mechanism for establishing trust across a multihop ABFAB federation
  - Where not all AAA Clients and Servers are connected via a single AAA server
  - Replaces current multihop AAA substrate that requires manual configuration at every hop
- Introduces a new ABFAB entity called the Trust Router
  - Trust router and KNP are combined to provide support for multihop federations

Trust router protocol



RADIUS substrate



- **Trust Router allows path selection through the AAA fabric**
- **Eliminates need for manual configuration at each hop**

Community of Interest (CoI)

- Conceptually: A set of users (Principals) and Services
- Technically: Set of IdPs, Relying Parties and Trust Routers

- Each CoI results in a separate routing tree, as paths must traverse nodes that are part of the right community
- Desire to support many Communities of Interest using a shared set of infrastructure and credentials
- Dynamic Trust Router makes it practical to support many Communities of Interest that come and go through a lightweight creation process

Trust Link

- A Trust Link represents an available KNP hop between a Trust Router and and another Trust Router or a AAA Server
- A Trust Link is an assertion that a Trust Router is willing to provide temporary identities to access another element in the ABFAB system
  - Another Trust Router
  - Or a AAA Server (Radius, RadSec or Diameter)
- Shown as a realm name and realm name (type), separated by an arrow
  - A->B(T) indicates there is a Trust Link from realm A to a Trust Router in realm B
  - ja.net -> oxford.ac.uk(R) indicates there is a Trust Link from ja.net to a AAA Server in oxford.ac.uk

Trust Path

- A Trust Path is a series of KNP hops that can be used to reach a AAA server in a destination realm
- Each hop across the substrate is called a Trust Link
- Shown as series of realms and types, connected by arrows
  - Currently defined types are Trust Router (T) or AAA Server (R)
  - Example: A -> B(T) -> C(T) -> D(T) -> D(R)

Trust Router Functions

- Trust Router Protocol
  - Distributes information about available Trust Links in the network
  - Calculates a tree of Trust Paths to reach target destinations
- Trust Path Query
  - Provide “best” path to a destination realm in response to queries from local RPs
- Temporary Identity Request
  - Provision temporary identities that RPs can use to reach the next hop in the Trust Path, in response to KNP requests from RPs

Trust Router Protocol

- Exchange information about Trust Links between Trust Routers
  - Trust Links are unidirectional and of a specific type
    - A -> B(T) does not imply A -> B(R), B -> A(T) or B -> A(R)
  - Realm names are not necessarily hierarchical, but they may be
    - example-u.ac.uk is not necessarily reached via .uk or .ac.uk
- Tree of available Trust Paths rooted in local realm is calculated by each Trust Router

Trust Router Messages

- Hello Message
  - Exchanged between neighboring Trust Routers to establish adjacency and perform authentication
- Trust Link Database Message
  - Used to send a full database when needed
- Trust Link Update Message
  - Used to send incremental database updates

- All messages encoded in JSON over TCP, with GSS-API-based security

Compact Tree Representation

- Trees (and subtrees) are represented as an ordered list of Trust Links (depth first traversal)
- Each entry contains
  - Index: Depth of this node in the tree
  - Target Entity: Type and Target of this link
  - CoIs: The CoIs to which this link applies
- Start of link is implied by location in the tree

Trust Path Query

- Generated by an RP to request a Trust Path to reach a AAA server in a destination realm
- When a Trust Path Query is received, the Trust Router:
  - Authenticates the RP, and checks local policy to determine whether or not to reply
  - Searches its tree of Trust Paths to find the best path to reach the destination
  - Returns the best path, if found, to the RP

Questions? Feedback?

- Questions about what we are proposing?
- Feedback on this proposal?

- Next Steps:
  - WG Chairs have suggested that we start with a problem statement document. Thoughts?
  - Who is interested in helping us with this work?
    - Review documents, contribute text, etc.